ARMY RESEARCH LABORATORY

Implementing a Virtual Private Network for a Mobile LAN Using DIRECWAY and OpenSSH

by Brian B. Luu and Richard D. Gopaul

ARL-TR-3389 **December 2004**

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Adelphi, MD 20783-1197

ARL-TR-3389 **December 2004**

Implementing a Virtual Private Network for a Mobile LAN Using DIRECWAY and OpenSSH

Brian B. Luu and Richard D. Gopaul
Computational and Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
December 2004	Final	FY03

4. TITLE AND SUBTITLE
Implementing a Virtual Private Network for a Mobile LAN Using DIRECWAY and OpenSSH

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Brian B. Luu and Richard D. Gopaul

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
Attn: AMSRD-ARL-CI-CN
2800 Powder Mill Road
Adelphi, MD 20783-1197

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-3389

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
2800 Powder Mill Road
Adelphi, MD 20783-1197

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES
Approved for public release, distribution unlimited.

14. ABSTRACT
Mobile Internet Protocol (IP) Local Area Network (LAN) is a technique, developed by the U.S. Army Research Laboratory, that allows a LAN to be IP mobile when attaching to a foreign IP-based network and using this network as a means to retain connectivity to its home network. This technique is a form of virtual private networking which enables a LAN to roam on the Internet. In this paper, we describe an enhanced version of Mobile IP LAN where a personal computer (termed a pass-through system) equipped with Hughes Network Systems (HNS) DIRECWAY (an upstream/downstream Internet service via satellite communications) and Secure Shell (SSH) software allows a LAN to be mobile in the United States. The pass-through system does no network routing (layer 3) but instead serves as a transparent (secure) bridge at layer 4 (transport layer) to link the mobile LAN and its home network. This bridging technique implemented on the pass-through system can be adapted to any system equipped with a network interface card, SSH software, and Internet access as a means to provide a VPN for a mobile LAN to its home network

15. SUBJECT TERMS
Mobile IP LAN, VPN, secure tunnel, OpenSSH, satellite communications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Brian B. Luu
Unclassified	Unclassified	Unclassified	UL	18	19b. TELEPHONE NUMBER (*Include area code*) (301) 394-3102

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

List of Tables

1. Introduction

The U.S. Army Research Laboratory (ARL) has developed and tested the Mobile Internet Protocol (IP) Local Area Network (LAN) protocol to support mobility for the Army on the digital battlefield. The Mobile IP LAN protocol (*1*) allows a LAN to be IP mobile without modifying its LAN IP configuration (such as IP address, network mask, broadcast address, etc.). Only the LAN default gateway (router) needs to adjust to accommodate the change in network connection. When the mobile LAN moves to a new location, i.e., a foreign network, Mobile IP LAN requires that the mobile router (mobile LAN default gateway) acquire an IP address at the foreign network in order to retain network connectivity for the entire LAN. To protect the network traffic of the mobile LAN traversing between the foreign network and the home network of the mobile LAN, we use Open Secure Shell (OpenSSH) software, a freeware version of Secure Shell (SSH) (*2*). By taking advantage of strong encryption, authentication, and tunneling (port forwarding) of the OpenSSH software, we create a secure tunnel to channel the network traffic of the mobile LAN between the mobile router and the home agent (a special node at the home network to redirect the mobile LAN network traffic). The Mobile IP LAN with OpenSSH technique is an implementation of a virtual private network (VPN) for a mobile LAN to roam on the Internet.

In this paper, we demonstrate the use of a middle (pass-through) system that allows a mobile LAN to take advantage of Hughes Network Systems (HNS) DIRECWAY, an upstream/downstream Internet service via satellite communications, and OpenSSH to create a VPN between the mobile LAN and home network. We also show the result of an experiment measuring the data transfer rate through a pass-through system using different Internet connection means (different data rates). The use of the pass-through system removes the requirement of the mobile router to obtain an IP address at a foreign network. This is because the mobile router is linked to the home agent through the Internet connection of the pass-through system. The pass-through system does no routing itself, but instead acts as a bridge at layer 4 (transport layer), between the mobile router and home agent, using only the local and remote port forwarding capabilities of OpenSSH. More importantly, the bridging technique implemented on the pass-through system can be adapted to any system equipped with a network interface card (NIC), SSH software, and access to the Internet. This allows a mobile LAN to roam to a very restricted foreign network environment, especially one that does not provide an IP address to the mobile router, has strict firewall rules (but allows SSH traffic), or uses private IP addresses (*3*) for the internal network.

2. Background

2.1 Mobile IP LAN With OpenSSH

In general, a LAN accesses the Internet through a default gateway (router). When the LAN, including its default gateway, moves to a different location (termed a "foreign network") and acquires a new connection to the Internet, all intra-LAN connectivity still behaves as normal. However, the inbound traffic for the LAN continues to be routed on the Internet to its home network (the autonomous system where the LAN belongs). Normally, this change in the LAN gateway connection results in the loss of all LAN Internet traffic. To maintain Internet connectivity, the LAN gateway, termed the "mobile router," establishes a link to a special node at the home network, termed the "home agent," to request its inbound Internet traffic be forwarded to the LAN at its new Internet connection. The home agent accepts the inbound traffic for the LAN and routes it through an IP tunnel (*4*) using an encapsulation mechanism, with the destination address at the new Internet connection of the mobile router. The outbound traffic of the LAN can be routed normally through the foreign network connection to the Internet (if the foreign network allows this) or through another IP tunnel from the mobile router to the home agent. In brief, to maintain Internet connectivity when the LAN is away from its home network, the network traffic of the LAN is redirected through IP tunnels whose end nodes are the home agent and the mobile router. The Mobile IP LAN protocol is implemented based on this concept. It requires two special nodes (a home agent and a mobile router) equipped with network routing software, tunneling software, and an IP address on the foreign network.

Hence, when IP mobile, a mobile LAN's tunneled network traffic must traverse one or more foreign networks that may not be trusted. This traffic could be subject to eavesdropping, interception, modification, or redirection by malicious nodes in these foreign networks. To protect network traffic passing through the tunnels, we use the port-forwarding feature provided by OpenSSH to provide a secure, bi-directional tunnel to carry the mobile LAN network traffic between the mobile router and the home agent. Port forwarding inherently takes advantage of the data encryption and data integrity features of OpenSSH to safeguard data flowing through the tunnel. OpenSSH also provides authentication that allows the mobile router and home agent to safely validate one another. Since OpenSSH software is found in the public domain, is available for most current operating systems, and is commonly used to provide secure network communications, OpenSSH is the software of choice. Figure 1 depicts a general overview of the operation of a mobile LAN using the Mobile IP LAN protocol with OpenSSH when at a foreign network.

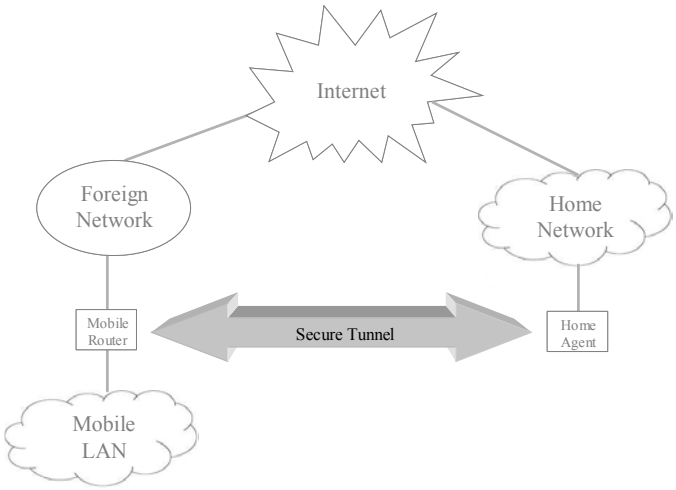

Figure 1. Mobile IP LAN with OpenSSH.

As described, the port-forwarding feature of OpenSSH provides a secure tunnel between the mobile router and home agent. To make use of this tunnel, a mechanism is necessary on both the mobile router and home agent systems that will pass all non-local mobile LAN traffic to the secure tunnel (port forwarded by OpenSSH). To implement this mechanism, we make use of the freeware TUN/TAP* device driver (*5*), available on the Linux, FreeBSD, and Solaris platforms, to create a virtual network device. The mobile LAN network traffic can then be routed to this virtual device. An in-house, ARL-developed program, STIP (Secure Tunnel Interface Program), reads network packets from the virtual device and passes them to the secure tunnel (*6*). The use of the combined virtual network device and STIP program is necessary on both the mobile router and home agent systems to properly implement the Mobile IP LAN with OpenSSH technique.

2.2 HNS DIRECWAY

HNS DIRECWAY provides two-way (upstream/downstream) Internet access using satellite communications. The upload network traffic from a DIRECWAY-enabled computer is sent up to an HNS geostationary satellite via a transmit modem and a satellite dish. The satellite, in turn, sends the traffic down to the HNS network operation center (NOC) where it is routed to the Internet as normal network traffic. Conversely, the download network traffic is routed through the Internet to the HNS NOC, where it is beamed up to the HNS satellite, transmitted down to the satellite dish and receive modem, and ultimately delivered to the DIRECWAY-enabled computer. The system running the HNS DIRECWAY service with business edition is assigned an IP address that is routable through the HNS NOC. The upload data rate is limited to 128 kbps, and the download data rate ranges from 400 kbps to 1.5 Mbps (*7*). HNS DIRECWAY

* Not an acronym.

allows a PC to be anywhere in the United States as long as the satellite dish can be aimed at the HNS satellite by line of sight. Currently, the device drivers for the DIRECWAY satellite modem are available only for Microsoft Windows platforms.

3. Technique and Implementation of Mobile IP LAN With OpenSSH Using a Pass-Through System

3.1 Technique

As previously mentioned, the Mobile IP LAN with OpenSSH technique can be used to securely route the network traffic of a mobile LAN roaming on the Internet. This comes with the condition that the mobile router of the mobile LAN can acquire a valid IP address at a foreign network where the mobile LAN roams. Problems arise when the mobile LAN moves to a location that has no Internet connection or a foreign network that cannot provide a routable IP address to the mobile router. In those situations, we can take advantage of the pass-through system technique using a PC (using Microsoft Windows operating systems) equipped with the DIRECWAY satellite communications service.

Since the DIRECWAY service can provide Internet access from anywhere in the United States, regardless of location, it can be used as a means for the mobile router to communicate with the home agent. The HNS network, where the DIRECWAY service accesses Internet, is the foreign network that the mobile LAN roams to. The PC running DIRECWAY, termed the pass-through system, should also contain a NIC to communicate with the mobile router in order to create a secure tunnel connecting the mobile router and the pass-through system. Since the link between the mobile router and the pass-through system is not visible to the outside world, private IP addresses can be used between them. The pass-through system will use the DIRECWAY service to communicate with the home agent to create another secure tunnel connecting the pass-through system and the home agent. The two tunnels are bridged at the pass-through system to create a transparent, seemingly complete secure tunnel linking the mobile router and the home agent. Figure 2 depicts the two secure tunnels joined at the pass-through system.

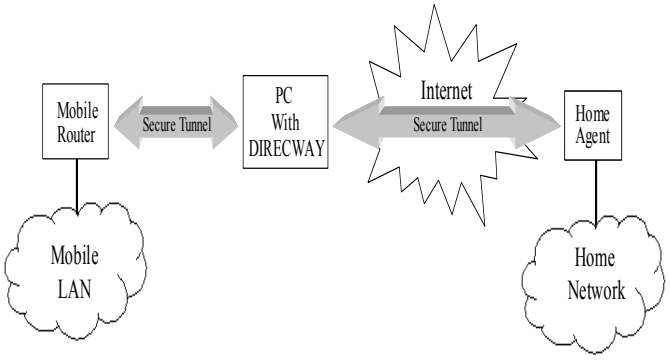

Figure 2. Secure tunnels joined at the pass-through system to connect the mobile router and home agent.

3.2 Implementation

In the implementation of a mobile LAN using the Mobile IP LAN with OpenSSH technique, we make use of a pass-through system to provide a connection between the mobile router and home agent systems. The pass-through system itself (in this implementation) is a PC running the Microsoft Windows 2000 operating systems, OpenSSH software, and the DIRECWAY satellite communication service (business edition). When the mobile LAN moves to a new location (where the mobile router has no direct connection to its home network), the pass-through system will initiate two secure tunnels by using OpenSSH to re-establish network connectivity. The first tunnel, between the pass-through system and the mobile router, uses the "remote forward" feature of OpenSSH. This feature gives the appearance that the flow of data is from the mobile router to the pass-through system. The second tunnel, between the pass-through system and the home agent, uses the conventional "local forward" feature of OpenSSH. This feature gives the impression that the data flow is from the pass-through system to the home agent. Although the appearance of data flow is from the mobile router to the pass-through system and from the pass-through system to the home agent, both tunnels allow bi-directional data flow. The tunnels themselves are actually OpenSSH forwarded ports that listen on a specific port of one system and forward all data received to another system at a specified port. To bridge two tunnels together at the pass-through system, the destination port of the tunnel between the mobile router and pass-through system must match the source port of the tunnel between the pass-through system to the home agent. For example, if the tunnel connecting the mobile router and the pass-through system listens on port 3000 of the mobile router and forwards data to port 4000 on the pass-through system, then the tunnel connecting the pass-through system and the home agent must listen to port 4000 on the pass-through system and forward data to a port (e.g., 2000) on the home agent.

Both the home agent and mobile router will use the STIP program to send and receive network data via the tunnels. The STIP program will use the TUN/TAP device driver to create a virtual network interface that the routing engine of operating systems can use to route the mobile LAN network traffic, through the tunnels, to and from the Internet. The routing tables of the mobile

router and home agent need to be adjusted to properly route the mobile LAN network traffic. Figure 3 shows the overall operation of the mobile LAN using the Mobile IP LAN with OpenSSH technique and a pass-through system with DIRECWAY Internet access.

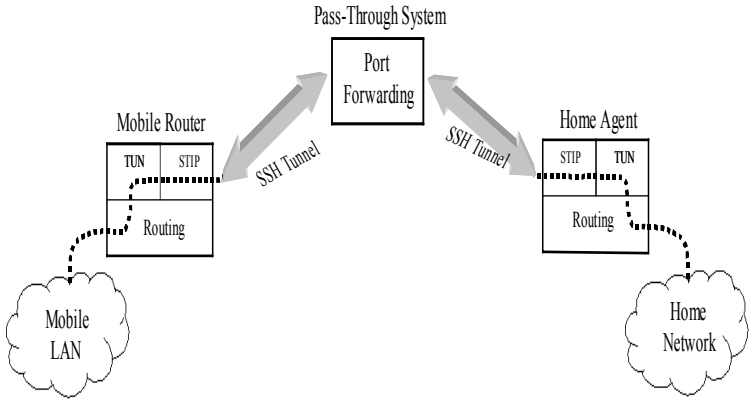

Figure 3. Mobile IP LAN with OpenSSH using a pass-through system.

4. Discussion

The use of a pass-through system with DIRECWAY removes the requirement of obtaining an IP address at a foreign network when implementing the Mobile IP LAN with OpenSSH technique. In fact, the IP address provided by the DIRECWAY service is a foreign IP address but is pre-known and location-mobile. In order to run the Mobile IP LAN with OpenSSH technique on the mobile router of a mobile LAN, the TUN/TAP device driver is required to create a virtual network interface. The TUN/TAP device driver is not available on the Microsoft Windows environment in which DIRECWAY is currently only available. Therefore, a PC running a Windows operating system and DIRECWAY is needed to create two secure tunnels and bridge them together to connect the mobile router and home agent. The connection of the mobile router and home agent provides a communication link to create a VPN for the LAN to be mobile in the United States. Although the pass-through system has two network interfaces (DIRECWAY and a NIC for communicating with the mobile router), it does not have to act as a router (passing network packets at layer 3, network layer). Indeed, the mobile LAN network traffic traversing the tunnels is passed at layer 4 (transport layer). Therefore, the operating system of the pass-through system can be any Windows version supported by the DIRECWAY software. It does not need to be a Windows server version.

The bridging technique of two SSH tunnels at the pass-through system running DIRECWAY can be adapted to any system furnished with a NIC, SSH software, and Internet access at any foreign network as a means to provide a VPN between a mobile LAN and its home network. Adapting the pass-through system technique makes the implementation of Mobile IP LAN for a mobile

LAN more flexible at very restricted foreign network environments, which may not provide an IP address, but instead allow the use of a system already connected to the network. Moreover, if the foreign network interface of the pass-through system uses a private IP address in a foreign network that implements network address translation (NAT) (*8*) for Internet access, the pass-through system technique still functions properly. This is because the secure tunnels are achieved using OpenSSH. Furthermore, the pass-through system at a foreign network can be restricted to allow only SSH network traffic, but can still bridge the mobile router and home agent systems together.

Since the pass-through system does no routing itself, there will be no leaking of mobile LAN network packets to the foreign network; only encrypted traffic of the mobile LAN will be visible to the foreign network environment. In addition, if the network link between the mobile router and pass-through system uses private IP addresses (a preferable and safe choice), then it is very difficult for any malicious nodes at the foreign network to attack the mobile LAN directly through the pass-through system because the pass-through system does not act as a router.

We conducted an experiment to measure the data transfer rate through the pass-through system between a node on the mobile LAN and a node on the home network. For encryption, we used the AES (Advanced Encryption Standard) encryption algorithm with a 128-bit key for OpenSSH. For Internet access of the pass-through system, we used the following connections: DIRECWAY, modem, and NIC (100-Mbps fastEthernet). The foreign IP addresses that were used for modem and NIC connection were from the University of Maryland. We used a 100-Mbps Ethernet NIC on the 10-Mbps LAN at the University of Maryland.

Only the speed at which the pass-through system connected to the Internet varied in all tests. The network link between the pass-through system and mobile router was always 100-Mbps Ethernet. We used Test TCP (TTCP), a freeware network performance evaluator (*9*), to measure the data transfer rates between a Host 1 in the mobile LAN and Host 2 at the home network. The TCP (transmission control protocol) transport method was used for data transfer in TTCP instead of UDP (user datagram protocol). Since the Internet connection of the pass-through system was not symmetric for upload and download data flow, we labeled the data transfer from Host 1 to Host 2 as the upstream data flow and the data transfer from Host 2 to Host 1 as the downstream data flow, as indicated in figure 4. For each transfer, we used 5 Mbytes of data.

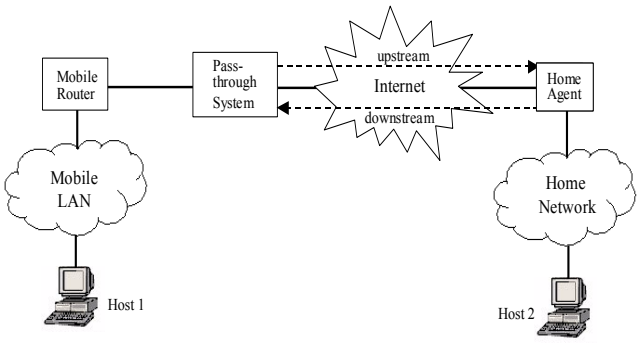

Figure 4. Upstream/downstream through a pass-through system.

All data rates (average) are tabulated in table 1. The results in table 1 also include measurements for the Mobile IP LAN with OpenSSH technique (without a pass-through system) for comparison with the pass-through system technique. Unfortunately, we could not evaluate the Mobile IP LAN with OpenSSH technique using DIRECWAY, since Mobile IP LAN requires the mobile router to run the TUN/TAP virtual network interface (not available on the Windows environments). Also, when implementing the Mobile IP LAN with OpenSSH technique using a modem for Internet access, the data transfer froze unpredictably. This problem did not occur in the pass-through system technique using a modem under the Windows environment. We suspect that this problem is related to the Linux modem device driver used in the Mobile IP LAN with OpenSSH technique using a modem.

Table 1. Data rates of transferring 5Mbytes of data.

Method	**Upstream Average (kbps)**	**Downstream Average (kbps)**
DIRECWAY (pass-through system)	22.49	76.68
Modem (pass-through system)	26.44	43.85
NIC (pass-through system)	1005.35	1561.83
NIC (Mobile-IP-LAN with OpenSSH)	1680.07	3051.88

The experimental data suggests that the file transfer time for modem and NIC in the pass-through method were stable and consistent for each direction (upstream and downstream). The data transfer time for DIRECWAY varied significantly (more than 100% for identical trials). This, however, is the nature of the DIRECWAY service, since all users share network bandwidth. The data rates, when using an NIC for Internet access, clearly indicate a higher data rate for the Mobile IP LAN with OpenSSH technique compared to the pass-through system technique (67% improvement for upstream and 95% for downstream) because there is less overhead (one SSH tunnel, less encryption) in the Mobile IP LAN with OpenSSH technique.

5. Conclusions

We have demonstrated the use of DIRECWAY on a PC as one way to alleviate the requirement of a foreign IP address to implement the Mobile IP LAN with OpenSSH technique for a mobile LAN to roam in the United States. The implementation of a pass-through system requires only an NIC, SSH, and a means of Internet access and does not depend on the operating system. It is more flexible to use the pass-through system to implement the Mobile IP LAN with OpenSSH technique for a mobile LAN at a restricted foreign network, since the mobile LAN does not need to directly attach to the foreign network. Furthermore, the VPN implemented by the pass-through system technique does not require a routable IP address at the foreign network interface of the pass-through system. The adoption of a pass-through system enhances the network security of a mobile LAN, albeit with a network data rate reduction for the mobile LAN compared to using the mobile router and acquiring a foreign IP address directly.

6. References

1. Luu, B. A Prototype Implementation of Mobile IP LAN. *Proceedings of Advanced Telecommunications & Information Distribution Consortium of ARL Federated Laboratory 5th Annual Symposium*, 211-215, March 2001.
2. Barrett, D.; Silverman, R. SSH, *The Secure Shell: The Definitive Guide*, O'Reilly & Associates, Inc., 2001.
3. Rekhter, Y.; Moskowitz, B.; Karrenberg, D.; de Groot, G. J.; Lear, E. "Address Allocation for Private Internets," RFC 1918, February 1996.
4. Perkins, C. "IP Encapsulation within IP," RFC 2003, October 1996.
5. "Universal TUN/TAP Driver," <http://vtun.sourceforge.net/tun>.
6. Luu, B.; Gopaul, R. Using OpenSSH to Secure Mobile LAN Network Traffic. *Proceedings of SPIE AeroSense 2002*, Vol. 4741, 54-61, April 2002.
7. "DirecWay 2-Way High Speed Internet Speed Tests," <http://www.macteks.com/sat/PDF/SpeedTest.pdf>.
8. Srisuresh, P.; Holdrege, M. "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663, August 1999.
9. "Test TCP (TTCP) Benchmarking Tool for Measuring TCP and UDP Performance," <http://www.pcausa.com/Utilities/pcattcp.htm>.

Distribution List

ADMNSTR
DEFNS TECHL INFO CTR
ATTN DTIC-OCP (ELECTRONIC COPY)
8725 JOHN J KINGMAN RD STE 0944
FT BELVOIR VA 22060-6218

OFC OF THE SECY OF DEFNS
ATTN ODDRE (R&AT)
THE PENTAGON
WASHINGTON DC 20301-3080

US MILITARY ACDMY
MATHEMATICAL SCI CTR OF EXCELLENCE
ATTN LTC T RUGENSTEIN
THAYER HALL RM 226C
WEST POINT NY 10996-1786

US ARMY ARDEC
ATTN AMSTA-AR-TD
BLDG 1
PICATINNY ARSENAL NJ 07806-5000

COMMANDING GENERAL
US ARMY AVN & MIS CMND
ATTN AMSAM-RD W C MCCORKLE
REDSTONE ARSENAL AL 35898-5000

US ARMY INFO SYS ENGRG CMND
ATTN AMSEL-IE-TD F JENIA
FT HUACHUCA AZ 85613-5300

US ARMY NATICK RDEC
ACTING TECHL DIR
ATTN SBCN-TP P BRANDLER
KANSAS STREET BLDG 78
NATICK MA 01760-5056

US ARMY SIMULATION TRAIN & INSTRMNTN CMND
ATTN AMSTI-CG M MACEDONIA
12350 RESEARCH PARKWAY
ORLANDO FL 32826-3726

HICKS & ASSOC INC
ATTN G SINGLEY III
1710 GOODRICH DR STE 1300
MCLEAN VA 22102

DIRECTOR
US ARMY RSRCH LAB
ATTN AMSRD-ARL-RO-D JCI CHANG
ATTN AMSRD-ARL-RO-EN W D BACH
PO BOX 12211
RESEARCH TRIANGLE PARK NC 27709

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI-C J GOWENS
ATTN AMSRD-ARL-CI-OK-T TECHL PUB (2 COPIES)
ATTN AMSRD-ARL-CI-OK-TL TECHL LIB (2 COPIES)
ATTN AMSRD-ARL-D J M MILLER
ATTN AMSRL-CI-CN B LUU (3 COPIES)
ATTN AMSRL-CI-SD R GOPAUL (2 COPIES)
ATTN IMNE-AD-IM-DR MAIL & RECORDS MGMT
ADELPHI MD 20783-1197

INTENTIONALLY LEFT BLANK.